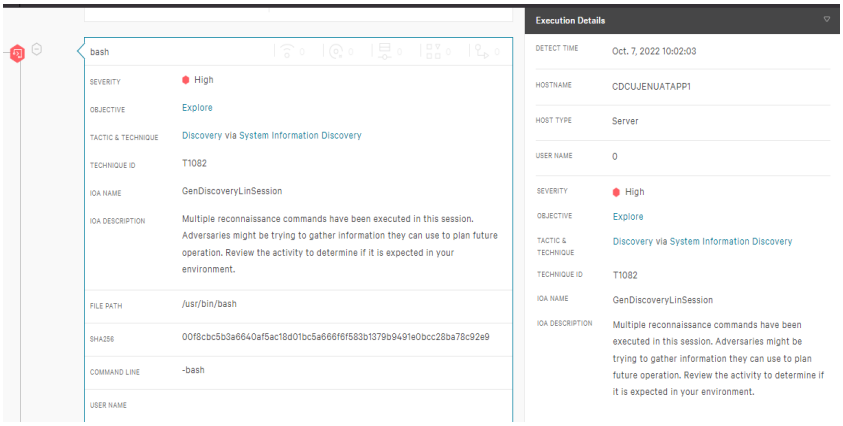
delhiveryTACTIC & TECHNIQUE : Discovery via System Information Discovery

IOA DESCRIPTION

Multiple reconnaissance commands have been executed in this session. Adversaries might be trying to gather information they can use to plan future operation. Review the activity to determine if it is expected in your environment.

Alert Triggered from Host **CDCUJENUATAPP1 - 10.40.17.64**



This is a CDC server. This Alert triggered for executing commands which are trying to get the details of ssh keys in linux server.

From Host timeline logs, we noted multiple bash commands executed by sshadmin user from IP 172.17.251.215 (**01VMCDCRHEL7**) and 172.17.8.90 (**CDCUNIXRHEL8**)

File Name: /usr/bin/logger
CommandLine: logger -p local3.info -t [audit sshadmin/93357 as jenkins/93535 on pts/4/(172.17.251.215):->:] /utxciserver 07/10/2022 10:03:22 cat /home/jenkins/.ssh/
SHA256: 6d4150739050d5d55ae6f18bd8dc8644cd60cc93c7c631f4424b04b7e533fc75
MD5: 9562e7513c84034b4e0e37b8b6db651c
PID: 93725
Parent ProcessId: 326034917884918206

File Name: /usr/bin/logger
CommandLine: logger -p local3.info -t [audit sshadmin/93357 as jenkins/93535 on pts/4/(172.17.251.215):->:] /utxciserver 07/10/2022 10:03:10 cd /home/jenkins/.ssh/
SHA256: 6d4150739050d5d55ae6f18bd8dc8644cd60cc93c7c631f4424b04b7e533fc75
MD5: 9562e7513c84034b4e0e37b8b6db651c
PID: 93669
Parent ProcessId: 326034917884918206

File Name: /usr/bin/logger
CommandLine: logger -p local3.info -t [audit sshadmin/92817 as sshadmin/92857 on pts/4/(172.17.8.90):->:] /home/sshadmin 07/10/2022 10:02:24 su - jenkins
SHA256: 6d4150739050d5d55ae6f18bd8dc8644cd60cc93c7c631f4424b04b7e533fc75
MD5: 9562e7513c84034b4e0e37b8b6db651c
PID: 93334
Parent ProcessId: 326034917467338090

Commands executed around the alert time are

from **172.17.251.215**

sudo su -

cd /home/jenkins/.ssh/

cat /home/jenkins/.ssh/

exit

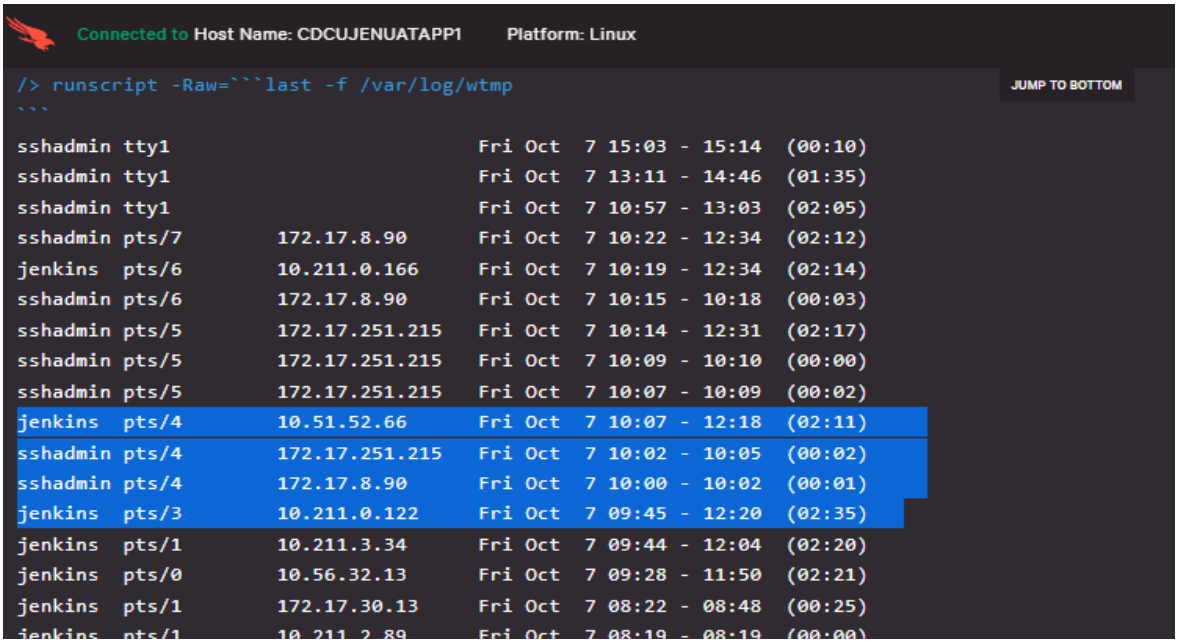
from **172.17.8.90**

su - jenkins

exit

Sudo su-

Logon history through script:

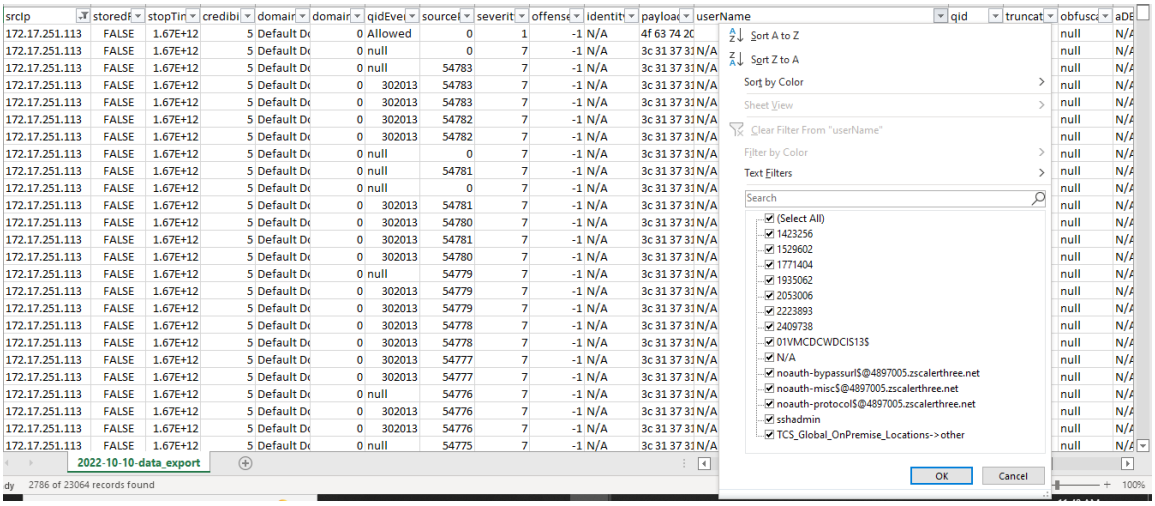


User name noted are sshadmin, Jenkins and root.

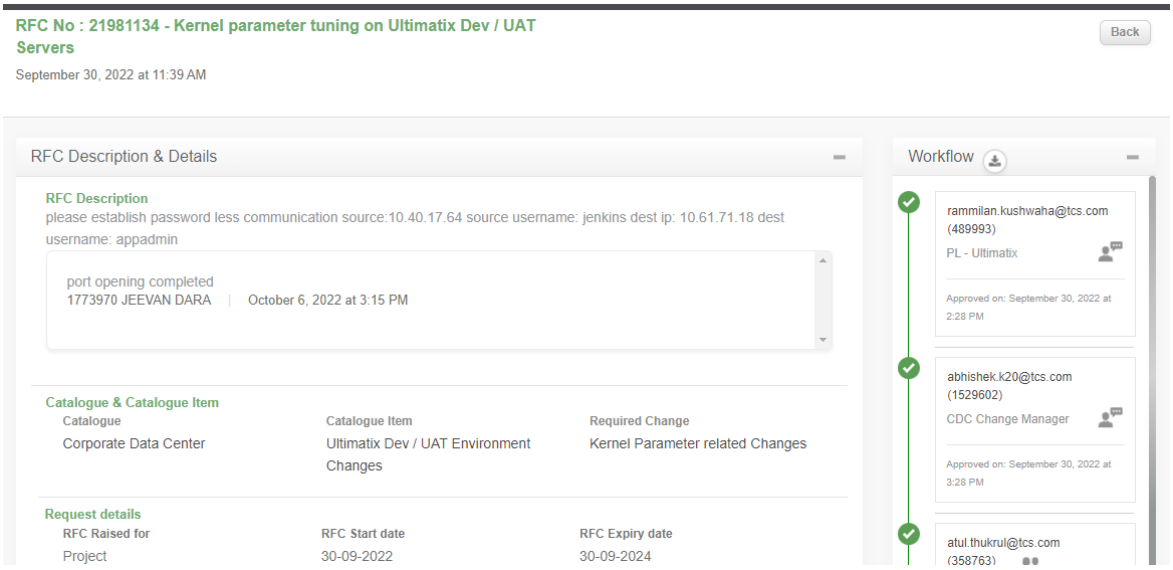
As checked timeline logs of 172.17.251.215 (01VMCDCRHEL7) and 172.17.8.90 (CDCUNIXRHEL8) we noted these are logged through another ssh session from VDI 172.17.251.113 (01VMCDCGDCIS001).

```
sshadmin pts/30    10.17.253.199    Fri Oct  7 12:51 - 15:05  (02:14)
sshadmin pts/29    10.17.253.199    Fri Oct  7 12:51 - 14:52  (02:01)
sshadmin pts/22    10.17.253.199    Fri Oct  7 12:51 - 14:52  (02:01)
sshadmin pts/25    172.17.251.113   Fri Oct  7 10:25 - 13:01  (02:36)
sshadmin pts/25    172.17.251.113   Fri Oct  7 09:57 - 10:05  (00:07)
sshadmin pts/22    172.17.251.113   Fri Oct  7 09:57 - 10:25  (00:28)
sshadmin pts/22    10.17.253.32     Fri Oct  7 06:09 - 06:38  (00:29)
```

Checked SIEM logs and host timeline logs for this IP and we able to find out user IDs login into this VDI



With this information the CDC team member, able to identify the source user and the activity performed which was related to establishing password less communication and they have shared the RFC details.



Hence concluded the case as False positive.